(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3420874 A1**

(51) Int. Cl. 4:
H04Q 7/02
H 04 L 11/26
H 04 B 17/00
H 04 K 1/00

(21) Aktenzeichen: P 34 20 874.7
(22) Anmeldetag: 5. 6. 84
(43) Offenlegungstag: 5. 12. 85

DE 3420874 A1

(71) Anmelder:
Licentia Patent-Verwaltungs-GmbH, 6000 Frankfurt, DE

(72) Erfinder:
Klostermann, Detlef, Dipl.-Ing.; Nettemann, Werner, Dipl.-Ing., 7900 Ulm, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Anordnung zur Kontrolle des Netzzugangs in Fernmeldenetzen

Verfahren zur Kontrolle des Netzzugangs innerhalb privater oder öffentlicher Fernmeldenetze, insbesondere Funktelefonnetze, zur Verhinderung bzw. zum automatischen Abbruch von Fernmeldeverbindungen, an denen nicht zugangsberechtigte oder manipulierte Teilnehmeranlagen beteiligt sind, durch Übertragung von Kontrollinformationen bei jedem Verbindungsaufbau. Zusätzlich zu einer offenen Teilnehmerkennung hat jede Teilnehmeranlage eine nur dem Netzbetreiber bekannte geheime Teilnehmerkennung abgespeichert. Bei einem Verbindungsaufbau wird die offene Teilnehmerkennung von der Teilnehmeranlage an eine Anlage des Netzbetreibers übermittelt. Anschließend sendet diese eine bei jeder Verbindung wechselnde Schlüsseleinphasung an die Teilnehmeranlage. Mit der Schlüsseleinphasung wird in der Teilnehmeranlage ein nur dem Netzbetreiber bekannter Schlüsselalgorithmus eingestellt, mittels dessen die geheime Teilnehmerkennung verschlüsselt wird. Die verschlüsselte geheime Teilnehmerkennung wird zur Anlage des Netzbetreibers übertragen, dort mit demselben Schlüsselalgorithmus wieder entschlüsselt und auf Übereinstimmung mit bzw. korrekte Zuordnung zur offenen Teilnehmerkennung überprüft. Bei Nichtübereinstimmung wird die Verbindung verhindert bzw. unterbrochen.

DE 3420874 A1

3420874

Licentia Patent-Verwaltungs-GmbH
Theodor-Stern-Kai 1
D-6000 Frankfurt 70

PTL-UL/B1/re
UL 84/76

Patentansprüche

1. Verfahren zur Kontrolle des Netzzugangs innerhalb privater oder öffentlicher Fernmeldenetze, insbesondere Funktelefonnetze, zur Verhinderung bzw. zum automatischen Abbruch von Fernmeldeverbindungen, an denen nicht zugangsberechtigte oder manipulierte Teilnehmeranlagen beteiligt sind, durch Übertragung von Kontrollinformationen bei jedem Verbindungsaufbau,
gekennzeichnet durch folgende Merkmale:

- zusätzlich zu einer offenen Teilnehmerkennung hat jede Teilnehmeranlage (Tln.) eine nur dem Netzbetreiber bekannte geheime Teilnehmerkennung abgespeichert;

- bei einem Verbindungsaufbau wird die offene Teilnehmerkennung von der Teilnehmeranlage (Tln.) an eine Anlage des Netzbetreibers (Ortsf.) übermittelt; anschließend sendet diese eine bei jeder Verbindung wechselnde Schlüsseleinphasung an die Teilnehmeranlage (Tln.);

...

- mit der Schlüsseleinphasung wird in der Teilnehmeranlage (Tln.) ein nur dem Netzbetreiber bekannter Schlüsselalgorithmus eingestellt, mittels dessen die geheime Teilnehmerkennung verschlüsselt wird;

- die verschlüsselte geheime Teilnehmerkennung wird zur Anlage des Netzbetreibers (Ortsf.) übertragen, dort mit demselben Schlüsselalgorithmus wieder entschlüsselt und auf Übereinstimmung mit bzw. korrekte Zuordnung zur offenen Teilnehmerkennung überprüft; bei Nichtübereinstimmung wird die Verbindung verhindert bzw. unterbrochen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die geheime Teilnehmerkennung durch eine nur dem Netzbetreiber bekannte Chiffrierung aus der offenen Teilnehmerkennung hervorgeht und vom Netzbetreiber zusammen mit einer Anordnung zur Verschlüsselung der Teilnehmeranlage (Tln.) zugesetzt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Übertragung der Schlüsseleinphasung und der verschlüsselten geheimen Teilnehmernummer während des Verbindungsaufbaus innerhalb des Fernmeldekanals im Frequenzmultiplex mit der Nutzinformation erfolgt, und daß zu diesem Zweck die Bandbreite der Nutzinformation kurzzeitig reduziert wird.

4. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß in der Anlage des Netzbetreibers (Ortsf.) die offene Teilnehmerkennung aus der Verbindungsaufbausignalisierung ermittelt, zwischengespeichert und für den Vergleich mit der entschlüsslten, dechiffrierten geheimen Teilnehmerkennung verwendet wird.

...

5. Anordnung zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche, gekennzeichnet durch folgende Merkmale:

- die Teilnehmeranlage (Tln.) weist ein Netzzugangsmodul (ZUM) auf, welches einen digitalen Speicher mit der geheimen Teilnehmerkennung und eine Anordnung zur Verschlüsselung enthält;

- die Anlage des Netzbetreibers (Ortsf.) weist eine Zugangskontrolleinheit (ZKE) auf; diese enthält einen Zwischenspeicher für die offene Teilnehmerkennung, eine Einrichtung zur Erzeugung einer Schlüsselphase, eine Einrichtung zur Entschlüsselung und Dechiffrierung der geheimen Teilnehmerkennung und eine Vergleichseinrichtung zum Vergleichen der offenen mit der geheimen Teilnehmerkennung.

6. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß das Netzzugangsmodul (ZUM) zwischen Handapparat (HA) und Sende/Empfangsgerät (MF) der mobilen Teilnehmeranlage (Tln.) steckbar ist.

...

Licentia Patent-Verwaltungs-GmbH
Theodor-Stern-Kai 1
D-6000 Frankfurt 70

PTL-UL/Bl/re
UL 84/76

Verfahren und Anordnung zur Kontrolle des Netzzugangs in Fernmeldenetzen

Die Erfindung betrifft ein Verfahren nach dem Oberbegriff des Anspruchs 1, sowie eine Anordnung zur Durchführung des Verfahrens.

Kontrollverfahren für den Zugang zu Fernmeldenetzen sind insbesondere für öffentliche Netze, die mit Benutzungsgebühren arbeiten, sinnvoll und bekannt. Der öffentliche Netzbetreiber hat für leitungsvermittelte Teilnehmeranlagen eine feste Zuordnung zwischen Teilnehmeranlage und Teilnehmerschaltung innerhalb der Einrichtung des Netzbetreibers über die zugeordnete Rufnummer des Fernsprechanschlußes (Teilnehmerkennung). Manipulationen sind hierbei unmöglich.

Bei nicht leitungsvermittelten Fernmeldenetzen oder Funkfernsprechnetzen muß die Teilnehmerkennung in der Teilnehmeranlage enthalten sein. Der Verbindungsaufbau wird

...

anhand der Teilnehmerkennung durchgeführt, und die Gebühren werden in der Einrichtung des Netzbetreibers registriert und der Teilnehmerkennung zugeordnet. Manipulationen der Teilnehmerkennung können somit auch die Gebührenzuordnung verfälschen.

Bei herkömmlichen Verfahren der eingangs genannten Art wird vom Netzbetreiber ein möglichst fälschungssicheres Element zur Festlegung der Teilnehmerkennung für die Teilnehmeranlage bereitgestellt und in sie implementiert. Ohne dieses Element ist die Teilnehmeranlage nicht betriebsfähig. Es sind auch Verfahren bekannt, die zusätzlich zur offenen Teilnehmerkennung eine Geheimnummer verwenden, die vom Netzbetreiber automatisch bei jedem Netzzugang zusammen mit der offenen Teilnehmerkennung kontrolliert wird.

Mit den o. a. Verfahren lassen sich Manipulationen z. B. zur Gebührenhinterziehung sicherlich erschweren, jedoch nicht verhindern, da die Kontrollinformationen auf dem Funkkanal abgehört und auf eine andere Teilnehmeranlage übertragen werden können.

Der Erfindung liegt die Aufgabe zugrunde, bei einem Verfahren der eingangs genannten Art den Netzzugang so zu kontrollieren, daß eine Manipulation der Teilnehmerkennung zum Zwecke des mißbräuchlichen Netzzugangs mit großer Sicherheit erkannt und der Netzzugang verhindert wird.

Die Erfindung ist im Patentanspruch 1 gekennzeichnet. Im Patentanspruch 5 ist eine Anordnung zur Durchführung des erfindungsgemäßen Verfahrens gekennzeichnet. Die weiteren Ansprüche beinhalten vorteilhafte Ausführungen der Erfindung.

...

Im folgenden wird die Erfindung anhand eines bevorzugten Ausführungsbeispiels für ein öffentliches Funkfernsprechnetz erläutert.

Betrachtet werden dazu ein Funkfernsprechanschluß als Teilnehmeranlage Tln., bestehend aus mobiler Funkanlage (Sende/Empfangsgerät) MF, Handapparat HA und Netzzugangsmodul ZUM gemäß FIG. 1 und ein ortsfester Funkfernsprechkanal Ortsf. als Anlage des Netzbetreibers, bestehend aus ortsfester Funkanlage OF, Überleiteinrichtung ÜLE, Zugangskontrolleinheit ZKE und Anschluß zum Selbstwähldienst SWFD (Telefonnetz) gemäß FIG. 2.

Die Netzzugangskontrolle wird von den Baugruppen ZUM und ZKE abgewickelt. Zwischen mobiler Funkanlage MF und Handapparat HA einer jeden Teilnehmeranlage wird ein Netzzugangsmodul ZUM und zwischen Überleiteinrichtung ÜLE und ortsfester Funkanlage OF eines jeden Funkfernsprechkanals wird eine Zugangskontrolleinheit ZKE geschaltet.

Sowohl die Zugangskontrolleinheit ZKE als auch das Netzzugangsmodul ZUM enthalten Verschlüsselungseinrichtungen mit identischem Schlüsselalgorithmus. Im ZUM ist außerdem eine geheime Teilnehmerkennung abgelegt.

Sowohl der Schlüsselalgorithmus als auch die geheime Teilnehmerkennung und ihr Hervorgehen aus bzw. ihre Zuordnung zur offenen Teilnehmerkennung sind nur dem Netzbetreiber bekannt.

Bei jedem Verbindungsaufbau, sobald die NF-Wege zwischen ZUM und ZKE durchgeschaltet sind, wird von der Zugangskontrolleinheit ZKE eine Schlüsseleinphasung bestimmt und

...

zum Netzzugangsmodul ZUM übertragen. Im ZUM wird damit dieselbe Schlüsseleinstellung wie in der ZKE vorgenommen. Mit dieser Schlüsseleinstellung wird im ZUM die geheime Teilnehmerkennung verschlüsselt und zur ZKE übertragen. Die ZKE entschlüsselt die geheime Teilnehmerkennung und dechiffriert sie zur offenen Teilnehmerkennung, die sie mit der beim Verbindungsaufbau abgespeicherten offenen Teilnehmerkennung vergleicht. Bei Übereinstimmung wird die Verbindung aufrechterhalten, andernfalls wird sie durch Trennsignalaussendung zwangsweise abgebaut.

Die Schlüsseleinphasung wird von der Zugangskontrolleinheit ZKE bei jeder Verbindung neu festgelegt und wechselt daher ständig.

Die geheime Teilnehmerkennung geht vorzugsweise durch eine nur dem Netzbetreiber bekannte Chiffrierung aus der offenen Teilnehmerkennung hervor. Alternativ dazu kann natürlich auch in den Anlagen des Netzbetreibers eine tabellarische Zuordnung zwischen geheimen und offenen Teilnehmerkennungen abgespeichert sein.

Zur Übertragung der Schlüsseleinphasung und der verschlüsselten geheimen Teilnehmerkennung wird der NF-Weg kurzzeitig über Filter aufgeteilt in einen eingeschränkten NF-Kanal und einen Signalisierkanal. Die Übertragung der Kontrollinformation für die Netzzugangsberechtigung erfolgt also noch während des Verbindungsaufbaus, so daß keine Verzögerung der Verbindung auftritt.

Das Verfahren bzw. die Anordnung gemäß der Erfindung erfordert wenig Aufwand und ist leicht in bestehende Fernmeldeanlagen, insbesondere Funktelefonanlagen nachrüstbar. Es ist absolut sicher gegen Mißbrauch, weil

...

- der Teilnehmer die geheime Teilnehmerkennung und ihren Zusammenhang mit der offenen Teilnehmerkennung nicht kennt und auch nicht aus dem ZUM herauslesen kann;

- der Teilnehmer den Schlüsselalgorithmus nicht kennt und nicht herausfinden kann, da die Schlüsseleinphasung ständig wechselt;

- wegen der verschlüsselten Übertragung der geheimen Teilnehmerkennung diese auf dem Funkkanal nicht abgehört und entziffert werden kann.

Das Bauteil ZUM mit eingespeicherter geheimer Kennung und Verschlüsselungseinrichtung wird vom Netzbetreiber bereitgestellt.

Nummer: 34 20 874
Int. Cl.[4]: H 04 Q 7/02
Anmeldetag: 5. Juni 1984
Offenlegungstag: 5. Dezember 1985

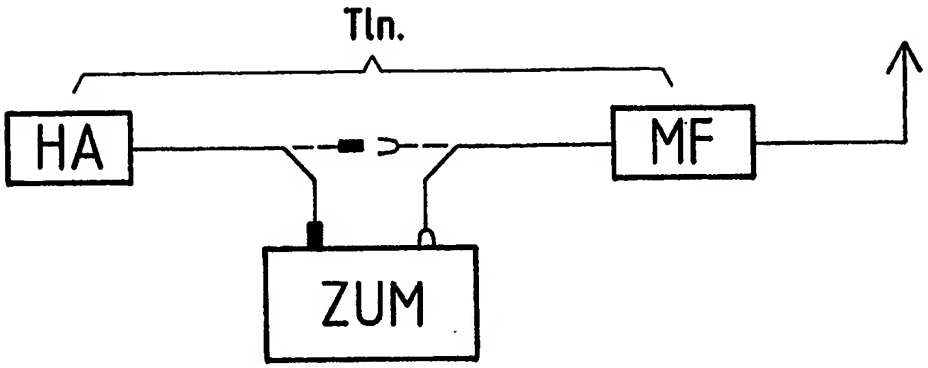

FIG. 1

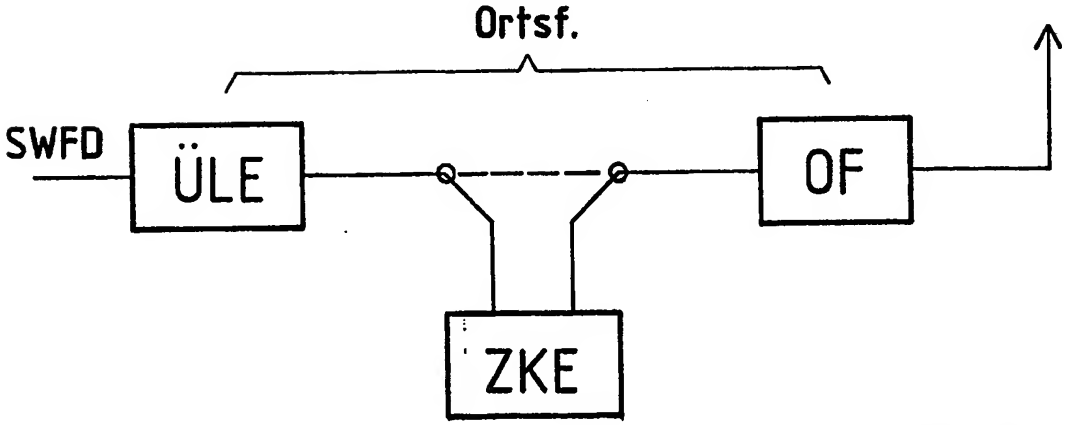

FIG. 2